# power up

## DISK & FILE

## Keep Your Mac Virus-Free

*by Kevin Savetz*

Computer viruses don't seem like a big deal—that is, until your Mac catches one. Once that happens, a virus may slowly corrupt your files, print strange messages, rename your hard drive, or even attempt to erase your disks. Relatively few viruses affect Macs: Macintosh users need to dodge somewhere around 55 viruses, compared to the thousands of strains that beset DOS and Windows users. Don't let that number lull you into believing that your computer is immune from infection. It only takes one virus—passed from a friend's floppy, downloaded from the Internet, or spread over the office LAN—to trounce the precious information stored on your Mac. An ounce of prevention is worth a pound of I-told-you-sos. Here are five steps to protect your Mac from viruses, plus one great Web site you should check out for more virus information.

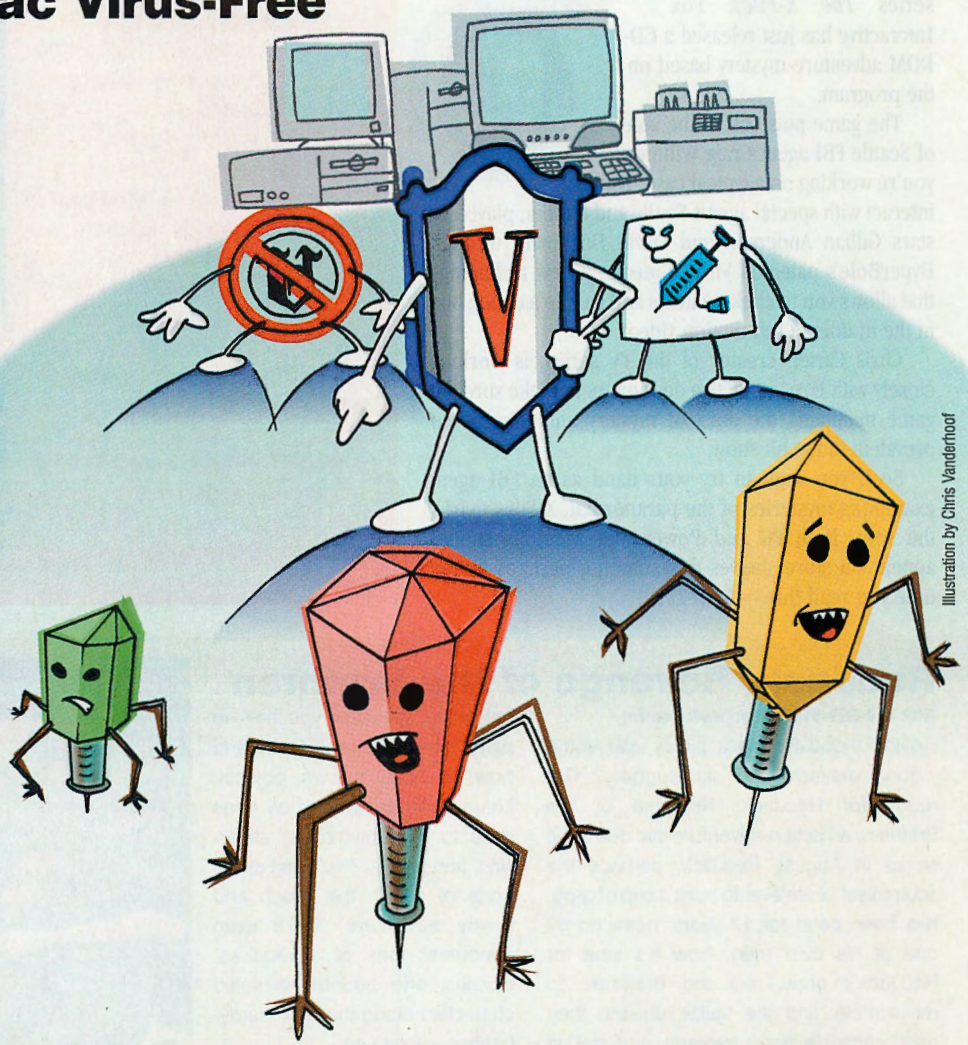
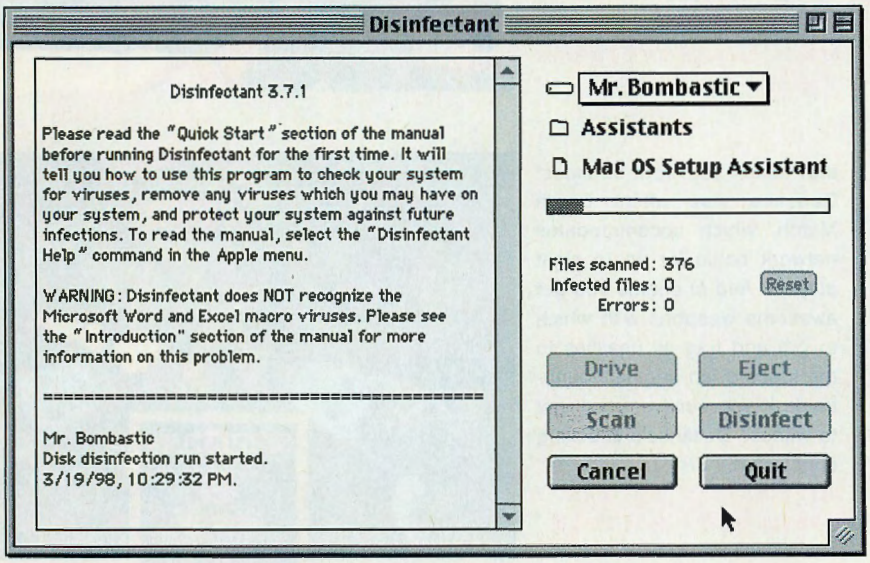
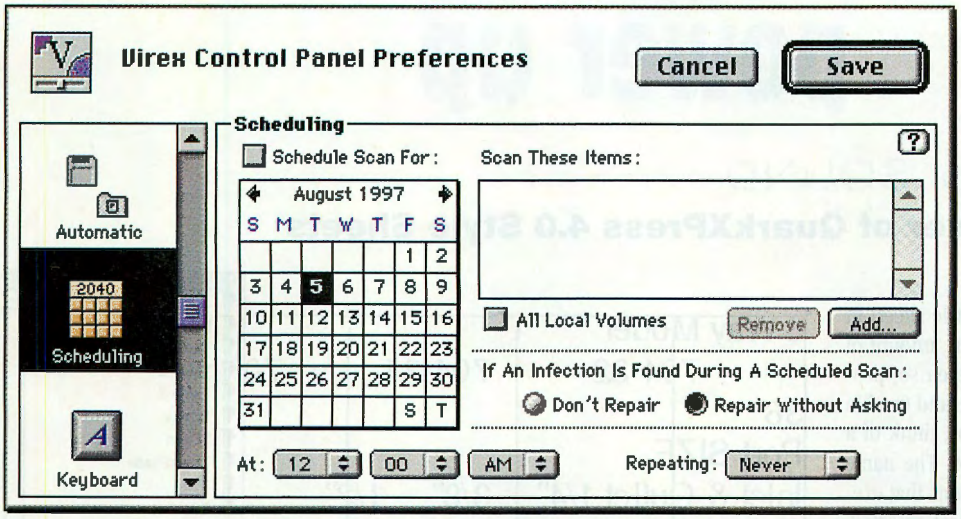



Illustration by Chris Vanderhoof


Disinfectant
Disinfectant 3.7.1
Please read the "Quick Start" section of the manual before running Disinfectant for the first time. It will tell you how to use this program to check your system for viruses, remove any viruses which you may have on your system, and protect your system against future infections. To read the manual, select the "Disinfectant Help" command in the Apple menu.
WARNING: Disinfectant does NOT recognize the Microsoft Word and Excel macro viruses. Please see the "Introduction" section of the manual for more information on this problem.
Mr. Bombastic
Disk disinfection run started.
3/19/98, 10:29:32 PM.
Mr. Bombastic
Assistants
Mac OS Setup Assistant
Files scanned: 376
Infected files: 0
Errors: 0
Reset
Drive
Eject
Scan
Disinfect
Cancel
Quit

### 1 Choose Antivirus Software

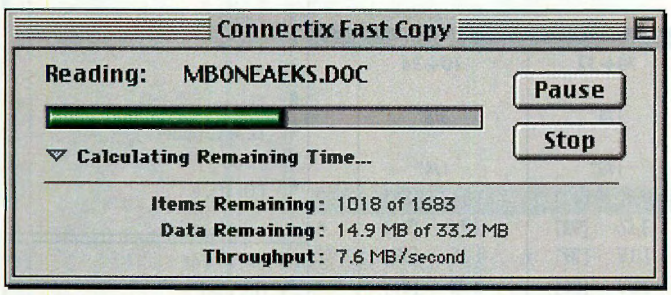
First things first: To keep your Mac free from infection, you'll need an antivirus utility. You can go two ways: Buy a commercial antivirus program, or choose a free one. If a free inoculation sounds like the way to go, Disinfectant (version 3.7.1) is the de facto standard. It does the basic job of scanning your system for viruses and removing any nasties it finds, but it doesn't cover all of the bases. Commercial antivirus programs tend to offer niceties lacking in bare-bones Disinfectant, and, sadly, Disinfectant will not be updated beyond its current version. Contenders in the commercial category are Symantec's Norton AntiVirus 5.0 for Macintosh (http://www.symantec.com/sam), Virex (http://www.drsolomon.com/products/virex/index.cfm), Dr. Solomon's AntiVirus Toolkit (http://www.drsolomon.com/products/avtk/ps_mac.html), and McAfee's VirusScan (http://www.mcafeemall.com/mall/mcafee/vsmacxfact.html).




**2 Check Your System for Viruses—and Get Rid of Them** After you've purchased or downloaded your antivirus utility, use it *regularly.* It thoroughly searches your Mac's hard disk for telltale signs of viruses. If it finds a virus, the software removes it—hopefully before the virus damages your precious data. Like that roll of dental floss you've pushed to the back of the medicine cabinet, antivirus software doesn't work unless you use it often. Running a thorough scan once a month should be fine for most people. Run it more often if you download many programs or exchange lots of disks with your associates, or if your Mac starts to act wonky. Every one of the programs listed above includes an extension or control panel that watches constantly for nefarious virus activity, even between scans. Make sure you enable that function for maximum protection.

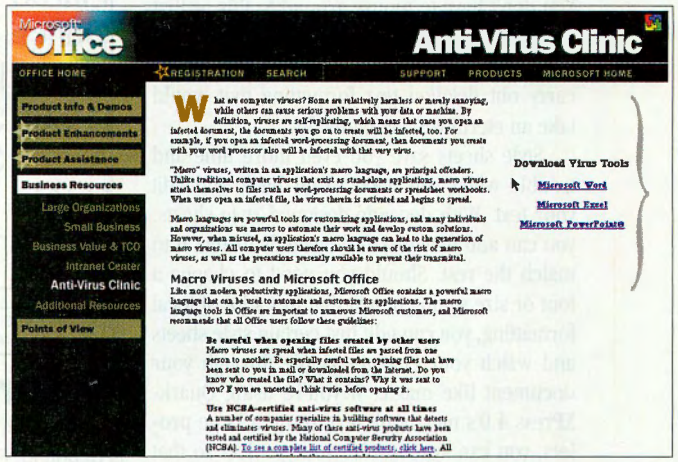
Version Tracker
Searching the Internet 24 hours a day for Mac updates
New Updates Search Updates Specials Links Sponsors Advertising Info
The Price/Performance Leader
Great low price
Fast Ethernet PCI Card
Farallon
Supercharge your Superfast G3
Freeware Freeware Beta Commercial upgrade Usfree commercial update or driver
Adobe Virtual Printer Plug-in - generate PostScript files even when no printer is connected 8.5.1 F 1/30/98
Connectix Virtual PC - Windows emulation software 2.0 - 1.0.1 C 3/16/98
Cosmopolitan Virtual Makeover - easy way to see how you'd look with different hair styles, eye color & more 1.0 C 1/1/98
Dr Solomon's Virex - virus protection software 5.8.1 C 10/1/97
Dr Solomon's Virex Virus Update - virus definitions for Virex 5.6 and later 4/1/98 U 3/31/98
La Cie Virtual Disk 2.0.3 U 1/1/97
Network Associates VirusScan - fix for handling the Word macro virus, WM.CAP 3.0.1 U 2/23/98
Network Associates VirusScan DAT Files - virus definitions for VirusScan versions 3.0 3/24/98 U 3/29/98

**3 Keep Your Antivirus Software Up to Date** In order to assure that no new strains can take residence in your Mac, keep your antivirus software up to date. Commercial antivirus tools make this easy: Their makers automatically send you updates—enhancements that tell the program how to identify new viruses—via the Internet or snail mail. If you use the freeware Disinfectant, don't bother looking for new versions, because there won't be any. You can also check with sites such as Version Tracker (http://www.versiontracker.com), which keeps track of the latest updates. Just search for the appropriate program or update name.




**5 Lock Out and Back Up** No antivirus software is foolproof. Happily, software is not your only defense. Viruses can't infect read-only media. If you walk around with floppies, Jaz disks, or other removable media in your pocket or purse, lock them to protect them from infection when you pop them into others' computers. A virus can't infect a medium it can't write to. Your ultimate defense—and you've heard this a thousand times—is to back up your data regularly. Don't just keep one backup of the most recent version; instead, rotate between several sets of back-ups. Keep them somewhere safe. Hide them in a place where no one ever goes. Put them in the pantry with your cupcakes. That way, even if your computer does manage to get infected, you can be sure that you've got at least one safe copy of your data.

**Kevin Savetz (http://www.savetz.com) is the keeper of Trivial.Net—trivia just for nerds—at http://www.trivial.net.**


Microsoft Office
Anti-Virus Clinic
OFFICE HOME
REGISTRATION SEARCH SUPPORT PRODUCTS MICROSOFT HOME
Product Info & Demos
Product Enhancements
Product Assistance
Business Resources
Large Organizations
Small Business
Business Value & TCO
Intranet Center
Anti-Virus Clinic
Additional Resources
Points of View
What are computer viruses? Some are relatively harmless or merely annoying, while others can cause serious problems with your data or machine. By definition, viruses are self-replicating, which means that once you open an infected document, the documents you go on to create will be infected, too. For example, if you open an infected word-processing document, then documents you create with your word processor also will be infected with that very virus.
"Macro" viruses, written in an application's macro language, are principal offenders. Unlike traditional computer viruses that exist as stand-alone applications, macro viruses attach themselves to files such as word-processing documents or spreadsheet workbooks. When users open an infected file, the virus therein is activated and begins to spread.
Macro languages are powerful tools for customizing applications, and many individuals and organizations use macros to automate their work and develop custom solutions. However, when misused, an application's macro language can lead to the generation of macro viruses. All computer users therefore should be aware of the risk of macro viruses, as well as the precautions presently available to prevent their transmittal.
Macro Viruses and Microsoft Office
Like most modern productivity applications, Microsoft Office contains a powerful macro language that can be used to automate and customize its applications. The macro language tools in Office are important to numerous Microsoft customers, and Microsoft recommends that all Office users follow these guidelines:
Be careful when opening files created by other users
Macro viruses are spread when infected files are passed from one person to another. Be especially careful when opening files that have been sent to you in mail or downloaded from the Internet. Do you know who created the file? What it contains? Why it was sent to you? If you are uncertain, think twice before opening it.
Use NCSA-certified anti-virus software at all times
A number of companies specialize in building software that detects and eliminates viruses. Many of these anti-virus products have been tested and certified by the National Computer Security Association (NCSA). To see a complete list of certified products, click here. All
Download Virus Tools
Microsoft Word
Microsoft Excel
Microsoft PowerPoint

**4 Trounce Annoying Macro Viruses Once and for All** A relatively new and exceptionally annoying type of virus is the *macro virus.* Normally viruses can travel only via infected applications. Macro viruses are the exception to the rule: They travel in the documents of programs with powerful scripting languages. Files in Microsoft Word and Excel are the most common macro virus hosts. Macro viruses are cross-platform—your Mac can catch a macro virus created on a PC. One way to deal with them is Microsoft's antivirus tool, available from http://www.microsoft.com/office/antivirus.asp. These scripts eradicate the most common Word and Excel macro viruses.

## SIDEBAR
## Virus help is online

A great place to find the latest information on Macintosh viruses is at Mac Virus (http://www.macvirus.com). This Web site, maintained by Susan Lesch, contains a ton of useful information about Macintosh system viruses, macro viruses, and other annoying pests. If you're looking for up-to-date virus information, check here early in your search. Mac Virus has an interesting article on the recently discovered Autostart 9805 Worm, which is the first worm to infect the Macintosh. To combat the Autostart 9805 Worm, Mac Virus recommends that you turn off the Enable CD-ROM AutoPlay in the QuickTime settings control panel. You can see if your Mac is infected by using the Finder's Find command to look for invisible files named DB, BD, or DELDB at your hard drive's root level, or those named Desktop Print Spooler, Desktop Printr Spooler or DELDesktop Print Spooler in the Extensions folder. Files named Desktop DB and Desktop Printer Spooler are legitimate files. The Autostart 9805 Worm affects PowerPC Macs only.